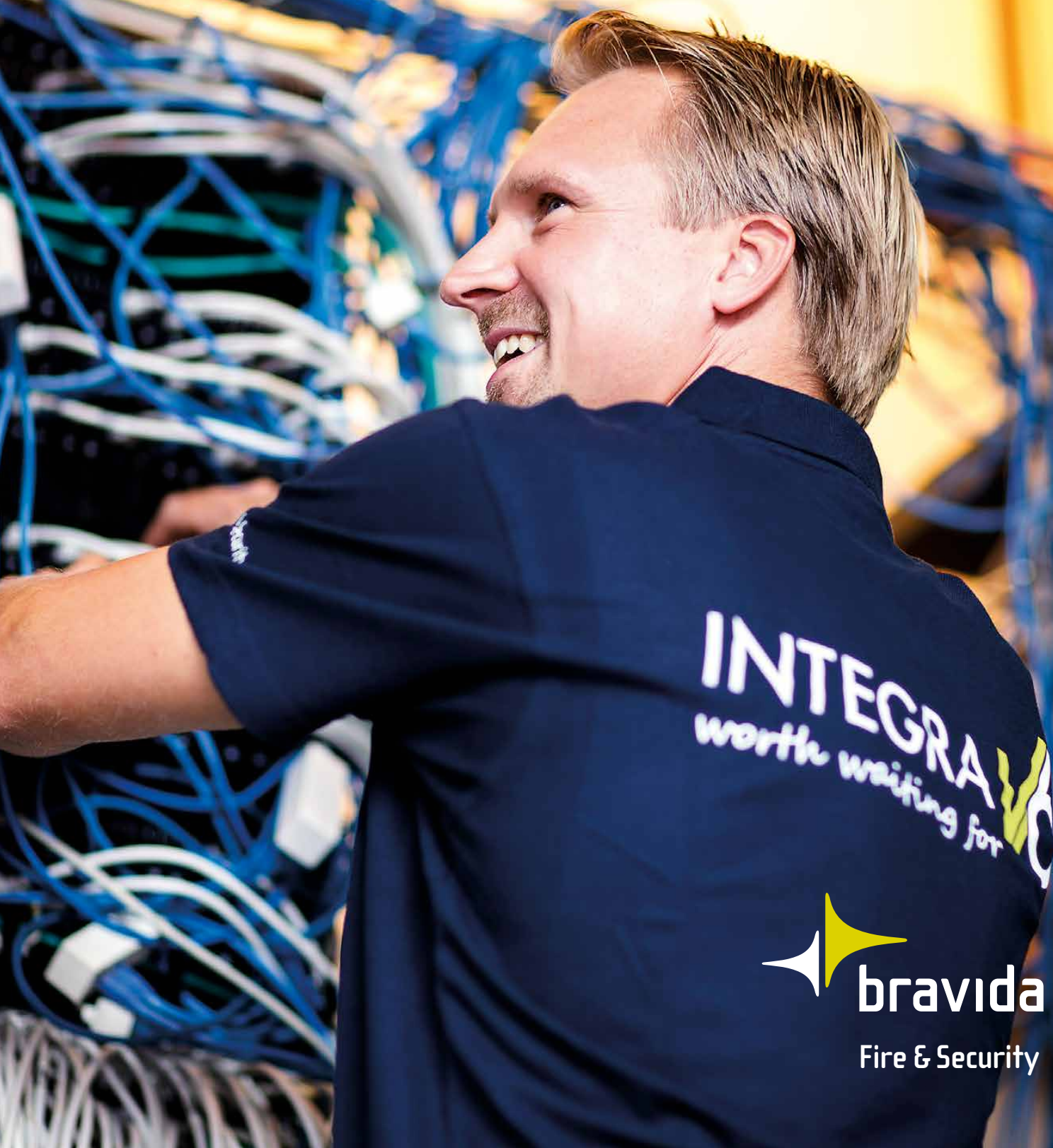


INTEGRA

SYSTEM DESCRIPTION





You can also find additional information at our website:
www.bravidafireandsecurity.com or www.systemhuset.com

System components	4
Keycards	8
Communications between PCs/servers and C-nodes	10
Software, platforms and functions	12
System security	14
Alarm collection, presentation and management	15
Special functions	16
Interfaces with other systems	17



BRAVIDA INTEGRA

Access control and alarm systems are essential for the implementation of security in commerce and industry as well as in public spaces. Getting the best possible security at the best price is just as important as getting a fully functioning system with the best possible functionality.

BRAVIDA INTEGRA is an integrated security system for access control, card production, burglar alarms, fire alarms, and CCTV surveillance that provides excellent security at a reasonable price.

BRAVIDA INTEGRA is simple to manage, and it is fully possible to expand the system with additional customised functions.

BRAVIDA INTEGRA is simple to integrate and external systems are easily managed through additional modules, such as OPC, Data Service and Alarm Service through our open interface Integra Easy Connect.

BRAVIDA INTEGRA has been developed to satisfy the market's stringent demands for functionality and ease of use.

This system description is intended to provide an overview of the system's components, as well as to demonstrate the options and solutions that Bravida Integra has to offer. For more detailed information, please refer to the user manual, consultant manual and the individual product sheets.

SYSTEM COMPONENTS

SOFTWARE

Bravida Integra – A scalable system

The software for Bravida Integra is scalable, can be modified and is capable of handling both large and small systems. The largest installations comprise thousands of door environments and alarm points, while the smallest systems may have only a few.

BRAVIDA INTEGRA **BASE**

For smaller systems that require a high level of security and user-friendliness, but have fewer door environments and alarm points.

BRAVIDA INTEGRA **PREMIUM**

For medium-sized to large systems or when you want to integrate other products via one of the many interfaces supported by Bravida Integra. Well-structured and easy-to-use alarm graphics can be used to visualise and manage alarm points.

BRAVIDA INTEGRA **ENTERPRISE**

For large systems that demand high performance and functionality. Well-structured and easy-to-use alarm graphics can be used to visualise and manage alarm points.

The system sizes above can be supplemented with a number of additional modules, such as CCTV, Data Service, Guard Report, Alarm Distribution, Alarm Monitoring, etc. More information about these modules can be found in separate product sheets.

Bravida Integra comprises the following programs:

Bravida Integra Server

Bravida Integra Server handles communications between PCs and substations. The program launches automatically, with Windows as the operating system.

Bravida Integra Client

Bravida Integra Client can be run on the same computers as the server software. The license for Client can be used by several computers, but only one user can use the program per license. Both the Premium and Base versions can be expanded with several licenses.

Bravida Integra Card Production

Bravida Integra Card Production Client is an additional module that enables card production. Card production is fully integrated and the program includes capabilities for taking photos, printing and designing end-cards.

Bravida Integra EasyConnect IEC

Bravida Integra EasyConnect is a program that serves as a link between external systems, such as HR systems, and Bravida Integra Server. DS communicates with 3rd party systems using the SOAP protocol and Webservice interface. IEC has the following features:

Cardholder: Create, Update, Read and Delete.

Card: Create, Update, Read, Delete, Attach to Cardholder, Detach from Cardholder.

Access level: Get List of Access Levels in Bravida Integra, Attach to Card Holders, Detach from Cardholders.

ACCESS CONTROL UNIT

Substation C-Node

One C-nodeG2 can handle up to 30 nodes for door environments and alarms or 30 wireless readers.

The node has an internal memory and database that handles local cards, access rights, time zones, security levels and other integral functions in the system. Information is always retrieved from the internal database. This means that all principal information and functionality is also available in offline mode. Memory management is implemented in the C-nodeG2 that enables you to split databases and store a huge number of access cards; 250.000 cards have been tested.

A C-nodeG2 can communicate with a host system on TCP/IP.



POWER SUPPLY WITH BATTERY (UPS)

The C-nodes and underlying units are supplied with DC power from a separate battery pack with two 40 Ah batteries, or larger if so required. This provides sufficient power for several hours of operation in the event of a power outage.



DOOR NODES AND ALARM NODES

Various nodes for door controls and alarms are connected to substations.

S-node

The S-node is a door alarm system suitable for high-security doors. It can also be used purely as an I/O unit that stores alarms and performs any actions required.

When the S-node is used as a door node, eight inputs and eight outputs are available and when it's used as an alarm node, eight inputs and two outputs are available.

The S-node communicates with a host C-node on LON bus FTT-10 and is sabotage-proof and is powered with 24 VDC and has an output with a 12 VDC supply for alarm detectors. The output can handle up to 1 A. All inputs can be defined as digital or double-balanced.



ComHub

The ComHub is a door box for 1:8 BCR-SW wireless readers. The ComHub communicates with a host C-node on RS485. ComHub is powered by 24 VDC.



Bravida Integra OPC Server

Bravida Integra OPC Server is a program that serves as a link between Bravida Integra Server and external systems.

Bravida Integra OPC Server enables interaction with external systems such as for opening doors, controlling areas, controlling alarm relays and reading statuses as alarm points.

OPC is an open standard for integration of systems. OPC (OLE for process control) is a standard specified by the OPC Foundation for communications between computers. This solution can be used together with a SCADA or HVAC-system.

Bravida Integra OPC Client

Bravida Integra OPC Client is a program that serves as a link between external systems and Bravida Integra Server. OPC Client converts OPC Tags into points that can be shown in Bravida Integra Client as standard objects. There are two kinds of objects that can be created in Bravida Integra Client – inputs (External Digital Input) and outputs (External Digital Output). This solution can be used together with a Integra and CCTV system.

Bravida Integra Alarm Service

Bravida Integra Alarm Service is a program that serves as a link between external systems, such as a paging system from Ascom, and Bravida Integra Server. This solution can be used between Integra and a Fire Alarm system.

CARD READERS

Bravida Integra includes a number of different card reader models (BCR) that support proximity keycards, such as EM Marin, Mifare and DESFire.

All other card models that support Wiegand or 'data-clock' interfaces can be used, including various types of biometric systems. All SmartCard readers are ready for NFC-reading.

BCR-SD AND BCR-S MINI PROXIMITY SMARTCARD READERS



BCR-SD

A BCR-SD card reader is included in the Bravida Integra access system for contactless card reading. The BCR-SD has a keypad for use in door environments that require an access code.

The card reader is equipped with a built-in antenna for card reading, a clearly visible keypad, LED indication, internal buzzer and convenient display for graphical symbols. The card reader is protected against sabotage in a sturdy ABS case with an EIA485 interface. The reader has Certification class SS-EN 50131-3:2009, grade 4.



BCR-S Mini

A BCR-S Mini card reader is included in the Bravida Integra access system for contactless card reading. This card reader has a sturdy design. The card reader features a built-in antenna for card reading, LED indication, internal buzzer and an EIA485 interface with moulded plastic encapsulation.

THE BCR-SD AND BCR-S MINI CAN READ MIFARE CLASSIC, MIFARE+ AND DESFIRE EV1 CARDS:

UID, sector reading and MAD with 4 or 7 bytes and Mifare Plus: UID, sector reading and MAD SL 0-3 with 4 or 7 bytes in the same readers and time.

Mifare DesFire can be used with ISO/IEC 14443-A unique serial numbers, 7 bytes and random IDs. Mifare DesFire cards can be used on multiple file system and fully compliant with ISO/IEC 14443A (part 1-4) using optional ISO/IEC 7816-4 commands security levels. The highest security level uses AES (Advanced Encryption Standard) encryption based on a 128-bit key length. This enables MIFARE DESFire EV1 to hold up to 28 different applications and 32 files per application in its flexible file system.

The card readers are generally mounted in a door environment with the S-node door control unit in a sub-assembly. The lightweight format is easy to position for ultimate user convenience.

NXP Semiconductor has developed the Mifare smart card technology. Mifare is based on the RFID technology that is currently used in fields such as transport, payment services and security, for example. The technology is especially useful due to its capability to save data in several sectors on a card. Reading can employ a serial number, a sector and MAD2.

Card readers with Mifare technology read cards at a distance of up to 5 cm from the reader (CR80 Cards). The read distance varies depending on the surroundings and any radio or metallic interference.

The cards for Mifare and Prox readers can be supplied as traditional cards or keyrings. Credit card-size proximity cards (CR80) can be combined with a magnetic strip and printed using a standard card printer.

BCR-SW WIRELESS PROXIMITY READERS FOR SMARTCARDS

BCR-SW

BCR-SW is the smart technology that enables mechanical locks to be wirelessly linked to Bravida Integra access control systems. The heart of BCR-SW is a short-range, wireless communications protocol, designed to link with an online electronic access system with a BCR-SW-enabled mechanical lock. A straightforward, easy and convenient way to add more monitored doors to a security system, BCR-SW allows for online access control and management, increasing both security and controllability.

BCR-SW IS COMPATIBLE WITH MIFARE & DES FIRE EV1 CARDS:

UID or sector reading, otherwise Mifare Plus: UID or sector reading.



BCR-PD AND BCR-P MINI PROXIMITY READERS FOR PROX EM MARIN



BCR-PD

A BCR-PD card reader is included in the Bravida Integra access system for contactless card reading. The BCR-PD has a keypad for use in door environments that require an access code.

The card reader is equipped with a built-in antenna for card reading, a clearly visible keypad, LED indication, internal buzzer and convenient display for graphical symbols. The card reader is protected against sabotage in a sturdy ABS case with an EIA485 interface. The reader has Certification class SS-EN 50131-3:2009, grade 4.



BCR-P Mini

A BCR-P Mini card reader is included in the Bravida Integra access system for contactless card reading. This card reader has a sturdy design. The card reader features a built-in antenna for card reading, LED indication, internal buzzer and an EIA485 interface with moulded plastic encapsulation.

BCR-PD AND BCR-P MINI ARE COMPATIBLE WITH EM MARIN:

4200 RO and 4550 RW in the same readers and time. The card readers are generally mounted in a door environment with the S-node door control unit in a sub-assembly. The lightweight format is easy to position for ultimate user convenience.

EM Microelectronic-Marin SA is a company in the Swatch Group that supplies chip technology suitable for access control. This technology has become an industry standard and is used by numerous card and reader suppliers.

Card readers with EM-Marin technology read the card at a distance of up to 12 cm from the reader. The read distance varies depending on the surroundings and any radio interference. Otherwise, the reader has the same properties as a magnetic card reader.

The cards for Mifare and Prox readers can be supplied as traditional cards or keyrings. Credit card-size proximity cards can be combined with a magnetic strip and printed using a standard card printer.

KEYCARDS

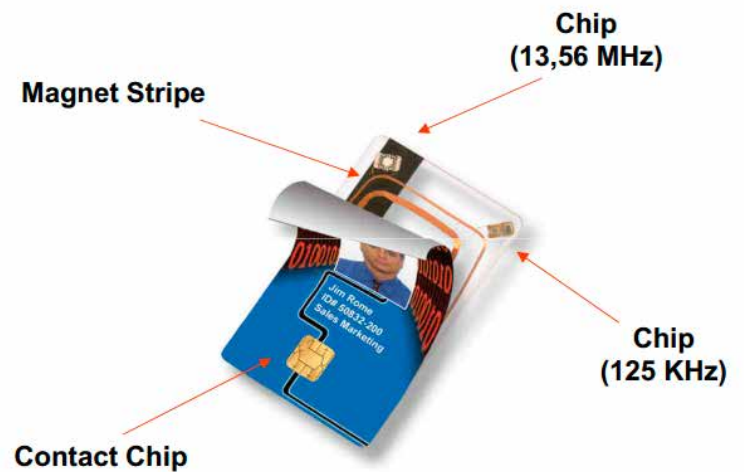
PROXIMITY CARDS, TAGS AND SMART CARDS (RFID)

This technology is based on radio signals. The card contains an integrated circuit that draws current from a coil in the card when the card is moved close to the reader. The card therefore has no battery and will continue to work provided there is no physical damage to the card or tag. Credit card-size cards are available. These can also be combined with a magnetic strip or smart card chip. Keyring tags of various designs are also available. However, tags do have a slightly shorter read distance.

BRAVIDA INTEGRA NO. 1 ON SMART CARDS

With Bravida Integra V6 a lot of effort has gone into developing a simple administrative solution for smart cards. Encryption keys for Mifare sector reading and MAD can be downloaded from a central location using encrypted communications and without any separate programming of card readers.

Bravida Integra V6 supports several encryption keys in the same card reader for Mifare sectors and MAD reading, which means that in addition to the customer's unique keys, the same system can also read cards from several suppliers, e.g. SITHS (county councils), ID06, etc.



BRAVIDA INTEGRA V6 SUPPORTS:

EM Marin: 4200 RO and 4550 RW

Mifare Classic: UID, sector reading and MAD with 4 or 7 bytes

Mifare Plus: UID, sector reading and MAD SL 0-3 with 4 or 7 bytes

Mifare DesFire EV1: UID and AES encrypted Application reading

MIFARE CLASSIC

Mifare Classic can be used with ISO/IEC 14443-A unique serial numbers, 4 or 7 bytes and random IDs. The security level uses CRYPTO1 encryption based on a 48-bit key length.

MIFARE PLUS

Mifare Plus can be used with ISO/IEC 14443-A unique serial numbers, 4 or 7 bytes and random IDs.

Mifare Plus cards can be used on multiple security levels. The highest security level uses AES (Advanced Encryption Standard) encryption based on a 128-bit key length. The lowest security level uses Crypto1.

To facilitate the migration process for existing infrastructures based on MIFARE Classic, the MIFARE Plus chip on its lowest security level is backwards compatible with MIFARE Classic.

Cards using chips on this lowest security level can be switched to a higher security level. Once a card is switched, it can only operate on that higher security level and cannot be switched back to a lower security level.

- **Security Level 0** – MIFARE Plus cards are pre-personalised with configuration keys, level-switching keys, MIFARE Classic CRYPTO1 and AES keys for the memory.
- **Security Level 1** – On this level, the cards are 100% functionally backwards compatible with MIFARE Classic 1K/4K cards. Cards work seamlessly in existing MIFARE Classic infrastructures.
- **Security Level 2** – Mandatory AES authentication. MIFARE Classic CRYPTO1 for data confidentiality.
- **Security Level 3** – Mandatory AES for authentication, communications confidentiality and integrity. Optional proximity detection (MIFARE Plus X only).

MIFARE DESFIRE

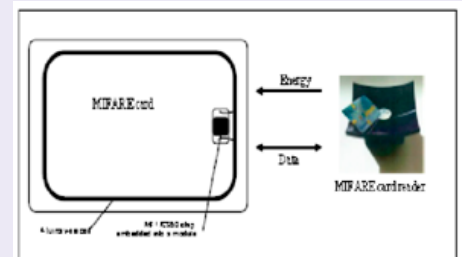
Mifare DesFire can be used with ISO/IEC 14443-A unique serial numbers, 7 bytes and random IDs.

Mifare DesFire cards can be used on multiple file system and fully compliant with ISO/IEC 14443A (part 1-4) using optional ISO/IEC 7816-4 commands security levels. The highest security level uses AES (Advanced Encryption Standard) encryption based on a 128-bit key length.

This enables MIFARE DESFire EV1 to hold up to 28 different applications and 32 files per application in its flexible file system

Comparison between MIFARE products

	MIFARE Classic	MIFARE Plus	MIFARE DESFire
Memory size	1KB, 4KB	2KB, 4KB	2KB, 4KB, 8KB
Protocol	ISO 14443-3	ISO 14443-3 ISO 14443-4	ISO 14443-4
File system	Fixed Structure	Fixed Structure	Flexible File System
Keys / crypto	2 CRYPTO1 keys per Sector	2 CRYPTO1 keys per Sector 2 AES Keys per Sector	Up to 14 AES keys per application
Transmission Security	Encryption	Encryption, Encryption + MAC, Plain+MAC	Encryption, Plain+MAC, Plain



COMMUNICATIONS BETWEEN SERVERS AND C-NODES

COMMUNICATIONS VIA ETHERNET/IP VPN

TCP/IP communications over a network is the best option when communications involve units at multiple geographic locations. The C-node is equipped with a network card for communications over Ethernet via TCP/IP protocols. The substation can then be connected to the PC network while it is online.

A fixed IP address is defined for the C-node.

SYSTEM DESIGN

Communication via LON (Echelon FTT-10)

LON bus communications are used for communications between the C-nod and sub-node (S-nod). This method is intended for situations when there are multiple substations within a relatively small area. The cable distances without using repeaters are comparatively long and cabling is easy. Network cards are not necessary.

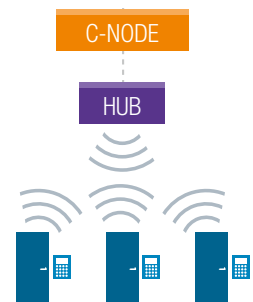
The C-node has a built-in communications port for LON communications with sub-nodes.

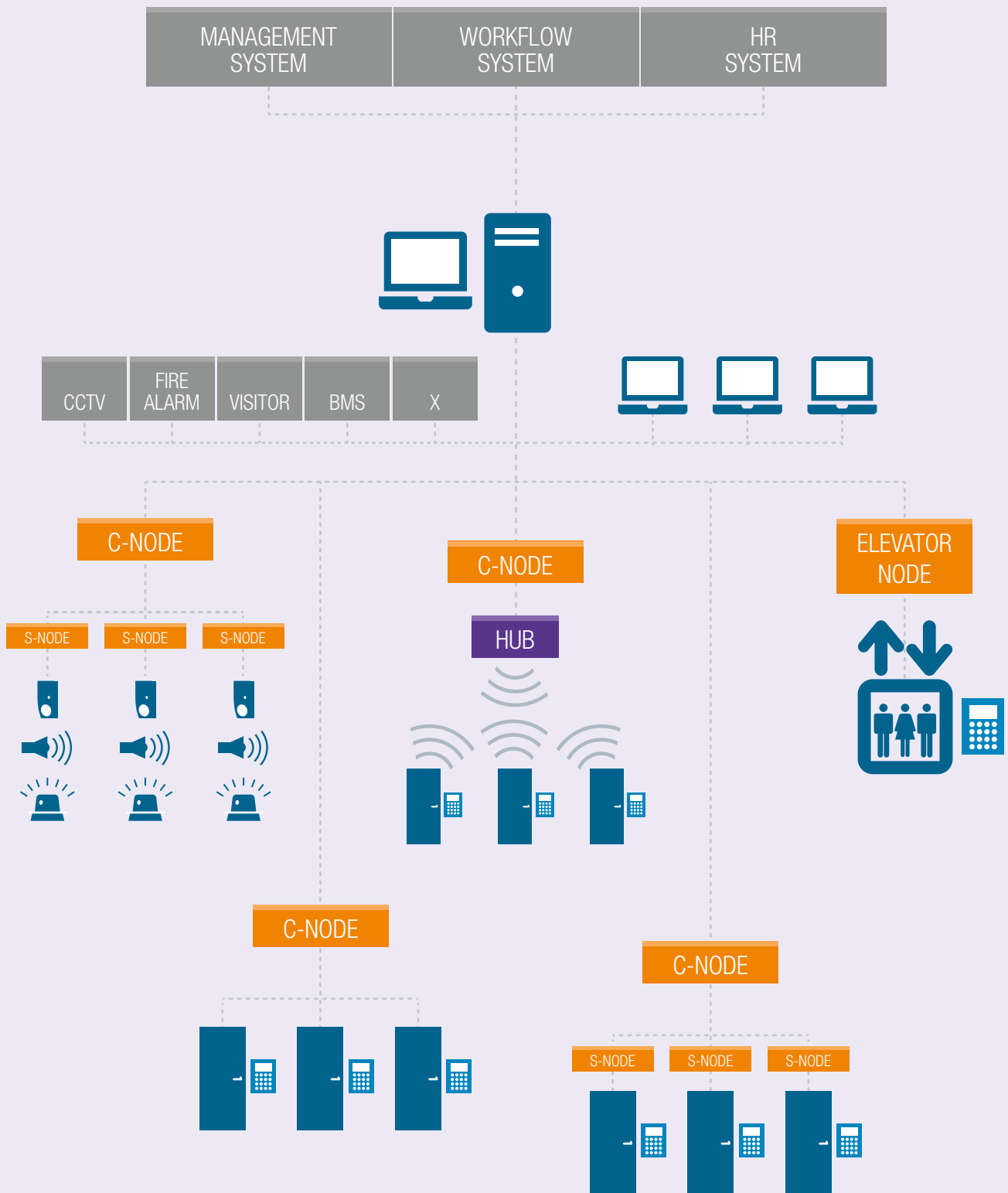
Communications via Wi-Fi

RS485 bus communications are used for communications between the C-node and radio hub for Wi-Fi readers. The cable distances without using repeaters are comparatively long and the cabling is easy.

The C-node has two built-in communications ports for RS485 communications.

Wi-Fi communications between a radio hub and BCR-SW readers comply with IEEE 802.15.4 and define the medium access control and the physical layer for WSN. It operates primarily in the 2.4-GHz band, using 16 channels. The bandwidth of each channel is 5 MHz. The MAC employs the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism. CCA (Clear Channel Assessment) is used in the physical layer to determine the channel occupancy. Distance between HUB and Wi-Fi readers can be up to 25 meters.





SOFTWARE, PLATFORMS AND FUNCTIONS

OPERATING SYSTEMS AND PROGRAMMING LANGUAGE

The system employs a standard PC platform and is compatible with Windows XP, Windows Vista, Windows 7, Windows 8 and Microsoft Server 2005, Microsoft Server 2008 and Microsoft Server 2012, 32- or 64-bit R2.



DATABASE

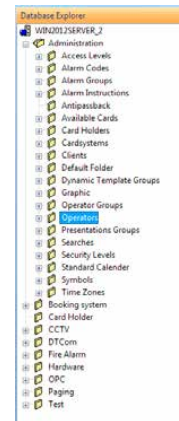
The system uses SQL Server as a database. The actual database is normally MS SQL 2012 Express. The full version of SQL Server can also be used. The database is run as a background program for Integra Server PC. Bravida Integra is compatible with MS SQL 2005, 2008 and 2012 64-bit R2.



SCREEN MANAGEMENT

Administrative tasks are performed in an environment similar to Windows Explorer. The structure comprises folders and objects in the same way as Windows Explorer. Objects represent all users, components and parameters present in the system. Folders with subfolders are created individually as required.

The system uses the 'drag-and-drop' principle to move objects between folders and to link objects. One example would be access permission for users.



ACCESS LEVELS

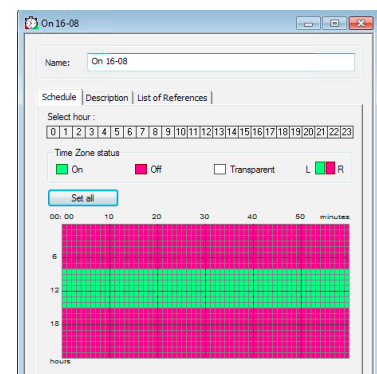
The access permissions in the system are based on a combination of card readers. Each card reader can be linked to a time zone for when a card with specific rights can be used. Access permission can also be linked to access the setting for 'bistable opening', when a card reader is used to set a door to permanent open mode.

TIME ZONES

Time zone settings are found in 'Day schedule for time zones' and 'Time zone'. In addition, the system also has an 'Analogue time zone' setting.

Day schedule for time zones

The day schedule defines periods within each 24 hours when a time zone will be on and off. One-minute intervals are used. The period is defined using the left and right mouse buttons for on and off respectively, and can be highlighted using the mouse cursor to change periods within the 24-hour period. The day schedule follows the predefined time period.

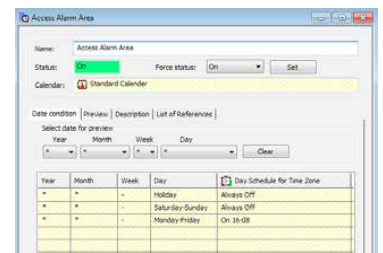


Time zone (comprising day schedule)

Time zones are used for normal time-controlled functions, such as restricted access to doors. A time zone is made up of several day time zones. A day time zone can last for several days for a single activity. This is determined in the field used to select the 'Day' period. The periods that can be selected are:

- Date
- Special days
- Monday–Friday
- Monday–Thursday
- Saturday–Sunday
- Holidays

A time zone is normally made up of Monday–Friday, Saturday–Sunday and a holiday.



Day	Day Schedule for Time Zone
Holiday	Always Off
Saturday-Sunday	Always Off
Monday-Friday	On 16-08

Calendar

The calendar function is used to specify the function of a time zone on an unspecified holiday.

Analogue time zone

An analogue time zone is used to limit functions by time, for instance, open doors with a time limit (e.g. 30 min) or 'buy time' when bypassing burglar alarms.

SECURITY LEVELS

The security level determines how the various card readers will function during the day.

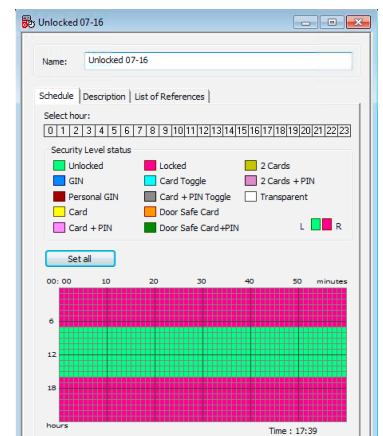
5.6.1 Security level

A security level is created in the same way as a time zone, but uses a day schedule for the security level. A security level can be used by one or more card readers.

5.6.2 Day schedule for security level

A day schedule for a security level determines how a card reader will function during the day. The options include:

- Unlocked:** Usually a main entrance during normal working hours
- Card:** Usually a department door during normal working hours
- Locked:** Usually a back door during evenings
- Card+PIN:** Normally all doors with a keypad during evenings/at night
- Card Toggle:** Usually an office door that is opened/closed regularly
- Card+PIN Toggle:** As above but with PIN code
- GIN:** Group code
- PGIN:** Personal code



ALARM COLLECTION, PRESENTATION AND MANAGEMENT

COLLECTING ALARMS

Alarm inputs on S-node

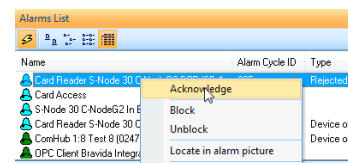
An S-node can be used as a combined door and I/O node or solely as an I/O node. When used solely as an I/O node, it has 8 double-balanced alarm inputs and 4 relay outputs.



ACKNOWLEDGE ALARMS ON AN ALARM LIST

An alarm list of unacknowledged alarms can be shown on the screen. Various colours are used to indicate status. Active alarms appear in red. Active acknowledged alarms appear in green, etc. For more information, please refer to the user manual.

Alarms are assigned a presentation group. The operator is assigned access to one or more presentation groups. This can be used for example, to alert maintenance personnel of technical alarms, and security guards of burglar alarms.



GRAPHICAL AND DYNAMIC ALARM PRESENTATION

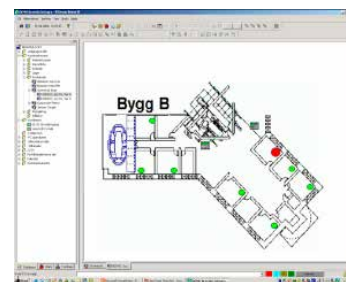
The system features an integrated graphical presentation of alarms. Alarms can be immediately displayed on a zone map, and doors can be opened remotely from the map.

MANAGEMENT OF ALARMS IN CARD READERS

An alarm zone that may comprise one or more alarm points can be defined for the system. Various actions can be implemented for card readers with keypads and displays.

- Alarm zones can be switched off and on
- 'Buy alarm bypass time'
- Transmission of status of current areas/zones
- Triggered alarms can be shown on the card reader display
- Inhibit points
- Etc.

Authorisation to handle alarms can be assigned to any card user and by any reader in the system.





SPECIAL FUNCTIONS

LIFT CONTROL

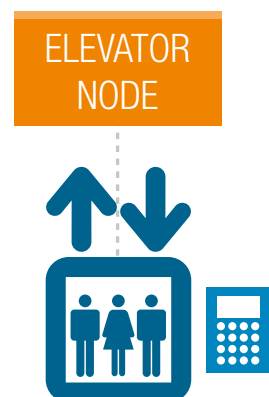
The standard C-node is used for access control in lifts. The solution makes it possible to define a virtual card reader for each floor. A physical card reader is installed in the lift. Virtual card readers are added at access levels, making it possible to assign different access levels to each floor if there are doors present.

When the card is read by the card reader in the lift, a relay is activated for each floor to which access is granted. The relays are connected to the lift control unit. The buttons for the floors to which the cardholder has access are now activated. The lift control solution can be used for several functions like one reader for several doors or cabinets.

SMS TO MOBILE PHONES

System messages can be sent to a mobile phone as SMS messages.

Messages are sent to third-party software using the SMTP protocol. The Omnigate software forwards alarms via a telephone with a SIM card.



INTERFACES WITH OTHER SYSTEMS

Bravida Integra can interact with other systems. We have chosen to integrate card production and alarm collection/management in Bravida Integra. In addition, Bravida Integra can be integrated with other systems using a variety of interfaces.

CCTV SYSTEMS

Bravida Integra can be integrated with a CCTV platform, such as Ethiris from Kentima, Milestone and Detec. This integration occurs during OPC communications between Bravida Integra and the CCTV platform.

One example of its use is if an indoor alarm on the Bravida Integra side is triggered, which in turn relays a message via OPC communications to the Ethiris CCTV platform, stating that the program may need to change the layout or display data from a PTZ camera.

Here is an example of a PTZ camera being triggered to start recording an event – in this case, an alarm from an IR detector.

OPC INTERFACE

Bravida Integra includes an OPC server and OPC client. This makes a number of solutions possible for interaction with other systems. One example is displaying messages from components and controlling components in the Integra system from a host presentation system.

OPC CLIENT & SERVER

With an OPC client, Bravida Integra can among other things, receive and display alarms, and handle instructions from other systems. With an OPC server, the Integra system can control functions in other systems. The OPC client is also used in integration with other system like CCTV platforms.

FIRE ALARMS

There is an interface in Bravida Integra for Autronica's fire alarm panels, for example. The idea behind this integration is that fire alarms can be presented and displayed as a part of Bravida Integra's alarm graphics. The alarms can also be displayed using Integra's presentation system.

DATABASE INTERFACES FOR HR DATABASES

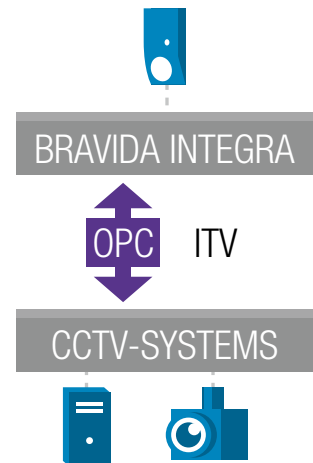
There is a program module that has been developed for exchanging data with other databases. For example, student registries or other personnel databases.

This function can automate and simplify card administration for large access systems with many users.

TERMINAL SERVER CLIENTS

Bravida Integra Client can be run on thin clients (Citrix Client) connected to a terminal server. The Bravida Integra Server software is installed on an external server/PC and connected to Citrix Terminal Server via a network.

Please contact us for more information about this solution.









+46 (0)8-602 30 00

Mikrofonvägen 28, SE-126 81 Stockholm Sweden

www.bravidafireandsecurity.com or www.systemhuset.com